NHS
Waltham Forest
Clinical Commissioning Group

NHS Waltham Forest

Clinical Commissioning Group

Information Governance Strategy

Author:	Zeb Alam, CCG IG Lead, (NELCSU) David Pearce, Head of Governance, WFCCG
Version:	4.0
Amendments to version 3.0:	Annual review and update: • Reference to Caldicott 2 assurance compliance • Referenced the new Caldicott work tasks in the IG Toolkit requirements • Reference to annual online IG training for Information Asset Owners (IAOs), Information Asset Administrator (IAA), SIRO, Caldicott Guardian and IG Lead • Updated Guidance on IG Incident reporting and the need to report IG Serious Incidents within 24 hours via IG Toolkit • Updated website link for IG Training website and IG incident reporting • Reference to Cyber Security and the IG Toolkit

	• Removed NHS form for IG incident reporting as this has been replaced by IG toolkit reporting of incidents • IG Strategy to be reviewed every 2 years unless national changes or changes in related legislation warrant an earlier review
Review date:	October 2017

Contents **Page**

1. Introduction

In the NHS, information is a vital yet potentially vulnerable asset, both in terms of the clinical management of individual patients and the efficient commissioning and management of services and resources. It plays a key part in clinical governance, service planning and performance management.

It is important that information is managed within a framework that ensures that it is efficiently managed and that appropriate policies, procedures and management accountability and structures are in place,

The following document outlines the strategy whereby NHS Waltham Forest Clinical Commissioning Group (WFCCG) meets its Information Governance (IG) responsibilities.

This strategy is a 3 year long term vision for Information Governance. The NHS has gone through a period of radical change. As a result, this strategy is supported by an annual improvement IG Toolkit plan focussing on changing compliance requirements, new legislation and areas specifically identified for improvement by the CCG.

The strategy is also supported by the Information Governance Policy which covers all aspects of holding, obtaining, recording, using, sharing and disclosing of data/information or records, held in a manual/paper or electronic format, by or on behalf of the CCG.

2. Information Governance (IG) defined

IG is the discipline of ensuring that the NHS complies with its statutory obligations to protect patient privacy including its obligation of ensuring confidentiality in the collection, processing and management of data and information.

It is defined by the requirements that the organisation is required to demonstrate compliance against an IG Toolkit Annual Assessment that includes the domains shown in Figure 1

Figure 1

3. Objectives

An outline of the high-level IG organisational objectives that WFCCG seeks to achieve is as follows:

- Comply with the relevant information privacy and confidentiality laws and regulations. This includes contractual requirements and internal policies on information and systems security and protection. Provide transparency on the level of compliance via the IG Toolkit
- To comply with the Department of Health Caldicott 2 compliance levels. The assurance is currently linked to the CCG IG work plan 2015/16 related toolkit requirements and will also be via the IG Toolkit submission at the end of March 2016. It is anticipated that more detailed guidance may follow from the Department of Health on the CCG compliance with Caldicott 2 during 2015-16.
- To comply with the Department of Health Cyber Security compliance levels. This will be via the IG Toolkit and by providing evidence on the related Cyber Security IG Toolkit requirements. This will be further linked to related toolkit requirements within the IG work plan 2015/16.
- Maintain information risk at acceptable levels and protect information against unauthorised disclosure, unauthorised or inadvertent modifications, and possible intrusions
- To minimise the risks arising from information handling processes and the subsequent damage or stress to an individual
- Address the increasing potential for civil or legal liability impacting WFCCG as a result of information breaches. Achieve this through efficient and effective risk management, process improvement and rapid incident management
- Provide confidence in interactions with WFCCG key providers, stakeholders and neighbouring CCGs. This also includes North East London Commissioning Support Unit (NEL CSU), NHS England, the Health and Social Care Information Centre (HSCIC) and other healthcare providers
- Create, maintain and continuously improve trust from customers and the public
- Provide accountability for safeguarding patient and other critical information
- Protect WFCCG reputation

4. Implementation

The implementation of this IG strategy, along with its associated IG policies and the IG Toolkit compliance plan will ensure that information is more effectively managed in the CCG. Every two years the IG strategy will be reviewed and a revised IG Toolkit plan will be developed to identify the key areas for a programme of continuous improvement.

5. Information Governance Plan

An overarching annual IG work plan will be overseen by the WFCCG Audit Committee. It will require active engagement with all areas of the organisation.

The plan will ensure compliance with the Information Governance Toolkit assessment to level 2 (satisfactory), as part of best practice and to maintain and build upon the previous submitted annual IG Toolkit score and link in with Cyber Security requirements and Caldicott 2. It is anticipated that there will be some IG toolkit requirements that may therefore achieve level 3 IG Toolkit scores but this is subject to CCG local resources and local IG reporting within the CCG..

A summary of the activities required to be undertaken is contained within the work plan in the CCG IG Overview Plan which is reviewed on a regular basis by the Senior Information Asset Owner (SIRO), on behalf of the Audit Committee. Please see IG work plan for more information.

The IG Toolkit report will be submitted on a quarterly basis to the Audit Committee and the Waltham Forest Governing Body will receive an annual IG update**.** Detailed planning will be included in the Information Governance Toolkit working documents and plans.

6. Roles and Responsibilities

Role	Summary	Who
	Has overall accountability and responsibility for governance within the organisation. Is provided with assurance, that all risks to the organisation, including those relating to information, are effectively managed and mitigated.	**Chief Officer**
Senior Information Risk Owner (SIRO)	Has overall responsibility for ensuring that effective systems and processes are in place to address the Information Governance agenda. • Foster a culture for protecting and using data. • Ensure information risk requirements are included in the Corporate Risk Management Policy. • To take ownership of the annual review of information flows and information asset registers and any advised recommendations. • Ensure Information Asset Owners (IAOs) undertake risk assessments of their assets. • Be responsible for the Incident Management process ensuring identified information security risks are followed up, incidents managed and lessons learnt. • Ensure IAOs and Information Asset Administrators have carried out their annual online Information Governance training. Provide a focal point for the management, resolution and/or discussion of information risk issues. • Ensure that the CCGs approach to information risk is effective in its deployment in terms of resource, commitment and execution and that this is communicated to all staff. • Ensure the organisation is adequately briefed on information risk issues. • Be accountable for information risk. • Has delegated authority from the Audit Committee to review and approve the IG Toolkit submission in cases where the Committee cannot meet to approve the pre-toolkit submission status. The SIRO roles and responsibilities are defined in Appendix A of the NHS Information Risk Management Guidance. The role holder will be supported and advised by the IG Team at NEL CSU	**Chief Financial Officer**
Caldicott Guardian	The role of the Caldicott Guardian is an advisory role, acting as the conscience of the organisation for management of patient information and a focal point for patient confidentiality & information sharing issues. It should be noted this is limited to where the CCG owns the data. • The Caldicott Guardian is supported in this role by the NEL CSU IG Team. • There are some new additional IG areas of Caldicott work in IG Toolkit version 13. These are mapped into the existing IG Work Plan for 2015-16.	**Director of Quality and Governance**

Role	Summary	Who
Information Asset Owners (IAOs)	All senior staff at Director level are required to act as Information Asset Owners (IAO) for the information assets within their remit. They will provide assurance to the SIRO that information risk is managed effectively for the information assists identified as within their remit. Key responsibilities of IAOs are to: • Ensure all Information Assets and flows of data within their remit are identified and logged ensuring each has a legal basis to be processed. • Identify, manage and escalate all information security (for example, dependencies and access control) and information risks as appropriate. • To complete mandatory annual IAO, IG online training related to the IAO role. The IAOs will be supported by Information Asset Administrators who will ensure the above takes place. The detailed roles and responsibilities are defined in Appendix A of the NHS Information Risk Management Guidance	**WFCCG Directors**
Information Asset Administrators (IAA)	Information Asset Administrators (IAAs) are the most senior individual user or direct users of systems and have an understanding as to how it works and how it is used • They will ensure there are procedures for using them, control access to them and understand their limitations. • To complete mandatory annual, IAA IG online training • To review the Information Assets and flows of data relating to their areas of work The detailed roles and responsibilities are defined in Appendix A of the NHS Information Risk Management Guidance	**Senior Managers**
Information Governance Lead at the CCG	CCG IG Lead working with CSU IG Lead to jointly cover and deliver the IG Agenda and IG Plan for the CCG. The IG Lead at the CCG acting as the first point of call for the CSU IG Lead and responsible for cascading information to colleagues in the CCG and for improving IG awareness and compliance in the CCG. • IG Lead at the CCG responsible for supporting the CSU in its (there will need to be an element of internal co-ordination to be done at WFCCG for this) Data Handling Review (covers Data Mapping) and for delivering key IG messages within CCG • To complete mandatory annual IG online training	**Head of Governance**
All Staff	All those working for the CCG have legal obligations, under the Data Protection Act, common law of confidentiality, and professional obligations, for example the Confidentiality NHS Code of Practice and professional codes of conduct. These are in addition to their contractual obligations which include adherence to policy, and confidentiality clauses in their contract. To complete mandatory annual IG online training	**All Staff**
Third parties	The same responsibilities apply to those working on behalf of the organisations whether they are volunteers, students, work placements, contractors or temporary employees. Those working on behalf of the organisation are required to sign a third party agreement outlining their duties and obligations.	**All third parties**

Role	Summary	Who
CSU IG Team	As part of the IG Service Level Agreement, the CSU IG Team members work with the CCG internal IG lead to help support the CCG in delivering the IG Strategy and , IG Toolkit, IG Policies and other IG related initiatives allowing the CCG to carry out business as a usual in a safe and secure manner. Where the CSU provides a service to the CCG, e.g. HR services, then the CSU IG Team provide the IG assurance related to the appropriate IG Toolkit areas.	

7. Key Policies

CCG to establish the following IG Policies to support this IG Strategy and ensure CCG staff abide by these:

- IG Policy
- Information Security Policy
- Information Management Policy (Records and Quality)
- Confidentiality and Disclosure of Information Policy
- Calendar, Email and Internet Policy

8. Policy, Protocol and Procedure Distribution

All employee based policies, protocols and procedures will be made available on the CCG intranet and will be highlighted in staff briefings.

Knowledge of the key details of Information Governance related policies will be tested through the use of the online Information Governance Training Tool (IGTT) l, and the use of staff surveys to test knowledge in particular areas.

9. IG Incidents

Reporting IG Incidents

All information incidents must be reported as soon as the issue is detected using the IG Incident Reporting Tool (see Appendix C).

The grading system for determining the severity of an incident is as used in the recently released HSCIC IG incident reporting guidance – see Appendix C. HSCIC – IG SIRI Checklist Guidance

These IG incidents cover:

- Near misses of information incidents
- Suspected information incidents (such as losses of data or breaches of confidentiality)
- Information Incidents (data losses and breaches of confidentiality)
- Patient Identifiable Data sent to the wrong individual
- Cyber related incidents. These include for example spoof websites, cyberbullying, and phishing emails. For more examples of cyber related incidents, please refer to the IG SIRI Checklist Guidance in the references/further guidance section. (see Appendix C)

If the incident is assessed at level two or higher, it must be reported by the appropriate Data Controller via the IG Incident Reporting tool as soon as is possible (usually within 24 hours of a breach being notified/identified locally) and with as much information as can be ascertained at the time. This web link opens the IG reporting tool guidance.

IG Incident Reporting Tool

The incident should be investigated in accordance with Waltham Forest CCG's Incidents and Serious Incidents reporting, Investigating and Management Policy.

Escalation of IG Incidents and Events

There is a requirement that certain incidents once assessed using the IG Incident assessment template be escalated within NEL CSU, Information Commissioners Office and Department of Health.

Other areas could potentially include customers, NHS England and other NHS organisations. This should be considered and continually reviewed in line with contractual requirements and the investigation process. Where this decision is to be taken it should be taken by the SIRO or where not available a director in conjunction with the Information Governance Team.

10. IT Security Incidents and Events

A number of the above incidents described above involve IT as a component and in such cases both IT and the CSU Information Governance Team should be informed. Where there is actual or suspected harm then the Information Incident should be reported along with any IT support requirements where required to the IT helpdesk.

The IT helpdesk will advise of any additional steps that are required, including initiating policy and procedure as outlined in the relevant Incident and Serious Incident and Investigation procedure.

Please see Information Security Policy for further details on which IT security incidents to report. The HSCIC IG – SIRI Checklist guidance in the references/further guidance section should also be referenced for further details on this (see Appendix C)

11. Routine staff briefings

The CCG will ensure that staff are up to date with IG Training and relevant legislation. Further information is provided in the IG Policy.

The staff bulletin and where necessary Information Governance specific messages will be sent to all employed staff. These will cover individual messages to support a wider picture of compliance and standards set to support this Strategy. Messages will be reviewed, updated if required and re-communicated at regular intervals to maintain consistent messages to staff.

12. Basic IG Training

All staff are required to complete and pass Information Governance on-line training on an annual basis to show a pre-requisite level of understanding. This for expedience will utilise the online information governance training tool as specified in section 6 – Roles and Responsibilities.

In addition to the annual mandatory Introduction to IG or IG: The Refresher training module (depending on whether staff have previously successfully completed the Introduction to IG training), identified staff as set out in section 6 (Roles and Responsibilities) to complete additional training appropriate to their duties. This will ensure that the CCG has the requisite IG awareness and controls in place to implement its IG Strategy.

The following staff have to carry out additional IG online annual training as part of their respective roles:

- Information Asset Owners (IAOs)
- Information Asset Administrators (IAAs)
- Senior Information Risk Owner (SIRO)
- Caldicott Guardian (CG)
- CCG Internal IG Lead

For more details of the IG training modules for the staff roles mentioned in section 6, refer to the IG Policy.

13. Support and advice

NEL CSU Information Governance Team will be a focal point and provide authoritative advice and guidance regarding the legal use of data in particular personal confidential data in line with reviewing national guidance and direction. They will be available via information.governance@nelcsu.nhs.uk

14. Appendices

Appendix A: Guidance for Reporting IG Related Incidents (see below)

Title:	Guidance for Reporting IG Related Incidents
Date:	27/08/2013
Submitted to:	Waltham Forest CCG
Author:	Mike Dunne

1. Introduction

1.1 Clinical Commissioning Groups have a responsibility for ensuring that all information governance related incidents that occur and that may breach security and/or confidentiality of personal confidential data, (PCD), are identified, reported and monitored.

2. Scope

2.1 This document outlines the procedure for reporting Information Governance related incidents. The identification and investigation of IG incidents will be done in line with the CCG's local incident procedure and the NPSA root cause analysis methodology. This document is limited to further reporting to regulatory bodies and data controllers. This is a requirement of the information governance toolkit and ISO 27001, Information Security Management.

2.2 This guidance will ensure that the CCG;

- Adheres to the processes and procedures for managing all IG SUIs
- That there is a consistent approach for evaluating all IG SUIs
- That early reports of IG SUIs are sufficient to provide appropriate escalation, notification and communication to relevant parties.
- Appropriate action is taken to prevent damage to patients, staff and the reputation of the NHS.
- All aspects of a SUI are fully explored and "lessons learned" are identified and communicated; and
- Appropriate corrective action is taken to prevent recurrence.

3. What is an Information Governance Related Incident?

3.1 An information governance related incident relates to the breach, theft or loss of personal confidential data (PCD), of patients or staff. This could be anything from users of computer systems sharing passwords to an email containing personal confidential data being sent to the wrong recipient.

4. Process for responding to IG Incidents

4.1 All incidents including IG related incidents should initially be reported using the CCG'S incident reporting template and sent by email to the Risk Manager.

4.2 If it is established that the incident is IG related, the Information Governance Lead will be notified that an IG incident has occurred. The severity of the incident should be established at the earliest opportunity as well as identifying who the owner/s of the data are and identifying the relevant parties to be informed of the incident.

4.3 The severity of the incident should be assessed in line with the Health & Social Care Centre's _IG Incident Reporting Tool guidelines.

4.4 Incidents assessed at level 2 or higher are classified as serious and must be reported to DH and the ICO through the Information Governance incident reporting tool, weblink attached._IG Incident Reporting Tool

This should normally be done within twenty four hours of becoming aware of the incident. For incidents assessed at level two and above a subsequent full root cause analysis investigation should be undertaken and an appropriate senior manager identified to lead on the investigation. There should also be appropriate input from relevant subject matter experts, IG, ICT, Security, etc.

4.5 Incidents assessed at level zero or one are deemed as low level incidents and should be processed in line with local policies and procedures. Organisations are not required to report level 0,1 incidents on the IG incident reporting tool.

5. Parties to be Informed of the Incident

5.1 When the identity of the data controller/s is established, the relevant data owner/s should be notified, irrespective of the level of incident.

5.2 **NHS England:** if it is established that NHS England is the data controller (joint or in common), the IG lead will be required to report the incident via the IG Toolkit if the incident is scored a level 2 or more.

5.3 **CCGs:** If the incident relates to individual funding requests, continuing health care, complaints, or other data for which the CCG is the Data Controller the relevant CCG

lead should be informed at the earliest opportunity so as to establish if the CSU or CCG should report the incident directly.

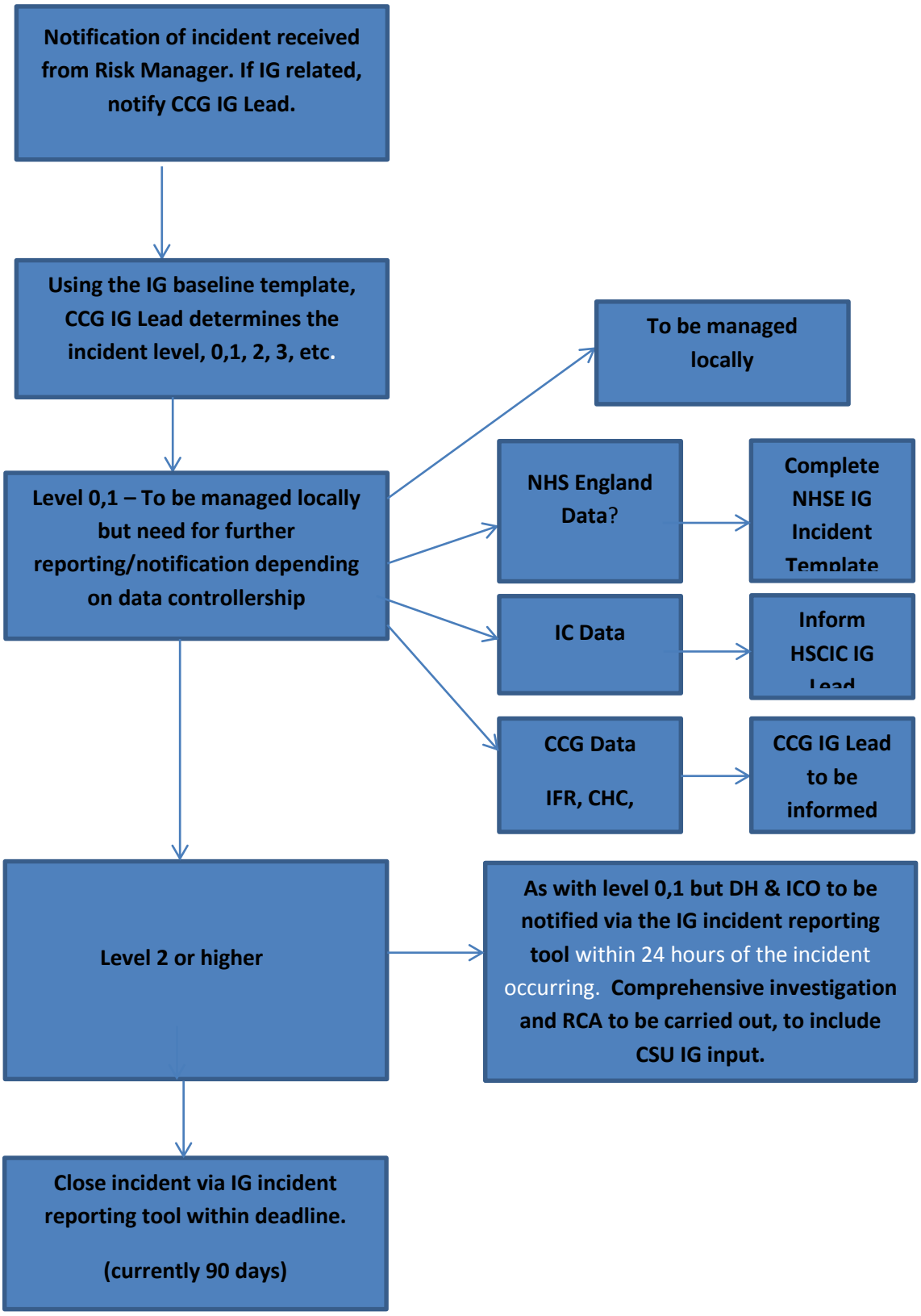
5.4 **HSCIC:** Where incidents relates to data supplied to the CCG by the Information Centre, they should be informed at the earliest opportunity.

6. Reporting Serious IG Incidents through STEIS

6.1 Provider organisations are still required to ensure that all serious incidents assessed at level two or higher, including IG incidents are reported through STEIS. This is to ensure that commissioners continue to be notified and ensure that they are managed effectively, in line with HSCIC guidance. However, responsibility for further reporting to other agencies rests with the provider IG Teams.

Appendix B

CSU IG Incidents Reporting Process - Flow Chart



Appendix C. Key Legislation and Guidance

Legislation

Access to Health Records Act 1990
Computer Misuse Act 1990
Data Protection Act 1998
Fraud Act 2006
NHS Act 2006
Regulation of Investigatory Powers Act 2000

References/Guidance

Appendix A of the NHS Information Risk Management Guidance
IG Training tool

HSCIC - IG SIRI Checklist Guidance and SIRI Assessment Tool

IG Incident Reporting Tool

IG Work plan 2015/16

Appendix D

Examples of Information Governance incidents that should be reported

- Finding a computer printout of patient details by a photocopier machine;
- Discovering that a fax containing PCD that was thought to have been sent to the correct recipient was incorrectly sent to the wrong person.
- An email containing PCD sent to the wrong person or sent using unencrypted email.
- Losing an unencrypted laptop computer with personal information on it;
- Giving information to someone who should not have access to it – verbally, in writing or electronically;
- Accessing a computer database using someone else's authorisation e.g. someone else's user id and password;
- Trying to access a secure area using someone else's swipe card or pin number when not authorised to access that area;
- Sending a sensitive e-mail to 'all staff' by mistake;
- Finding a colleague's password written down on a 'post-it' note;
- Discovering a 'break in' to the organisation;
- Finding confidential waste in a 'normal' waste bin;
- Coming across fake websites when using the internet for work issues;
- Phishing emails sending emails which appear to be from reputable companies in order to get individuals to reveal personal information, such as passwords and credit card numbers, online.

Appendix E: Equality Analysis

This is a checklist to ensure relevant equality and equity aspects of proposals have been addressed either in the main body of the document or in a separate equality & equity impact assessment (EEIA)/ equality analysis. It is not a substitute for an EEIA which is required unless it can be shown that a proposal has no capacity to influence equality. The checklist is to enable the policy lead and the relevant committee to see whether an EEIA is required and to give assurance that the proposals will be legal, fair and equitable.

The word proposal is a generic term for any policy, procedure or strategy that requires assessment.

	Challenge questions	Yes/ No	What positive or negative impact do you assess there may be?
1.	Does the proposal affect one group more or less favourably than another on the basis of:	No	
	▪ Race		
	▪ Ethnic origin (including gypsies and travellers, refugees & asylum seekers)		
	▪ Nationality		
	▪ Gender		
	▪ Culture		
	▪ Religion or belief		
	▪ Sexual orientation (including lesbian, gay bisexual and transgender people)		
	▪ Age		
	▪ Disability (including learning disabilities, physical disability, sensory impairment and mental health problems)		
2.	Will the proposal have an impact on lifestyle? (e.g. diet and nutrition, exercise, physical activity, substance use, risk taking behaviour, education and learning)	No	
3.	Will the proposal have an impact on social environment? (e.g. social status, employment (whether paid or not), social/family support, stress, income)	No	
4.	Will the proposal have an impact on physical environment? (e.g. living conditions, working conditions, pollution or climate change, accidental injury, public safety, transmission of infectious disease)	No	
5.	Will the proposal affect access to or experience of services? (e.g. Health Care, Transport, Social Services, Housing Services, Education)	No	

An answer of 'Yes' to any of the above question will require the Policy lead to undertake a full Equality & Equity Impact Assessment (EEIA) and to submit the assessment for review when the policy is being approved.